Remarks/Arguments

Claims 1-31 are pending. No amendments have been made to the claims.

Claims 10 – 28 and 30 – 31 are rejected under 35 U.S.C. § 101

Applicant respectfully traverses this rejection for at least the following reasons.

Independent claim 10 expressly recites a machine and a transformation and *when taken as a whole*, is directed to statutory subject matter. Independent claim 10 expressly recites that the method is operable at a receiving device that is in communication with a network. The following is the preamble of claim 10 which recites a receiving device which is *a machine that implements the claimed steps*.

> "A method, **operable at a receiving device** located at a remote site in communication with a network having at least one server and a content requester..." (emphasis added).

Furthermore, independent claim 10 recites a transformation. In particular, the last step of claim 10 recites the transformation of descrambling a second information item with a content key. The second information item was received scrambled (the first receiving step in claim 10). The method clearly recites the transformation from scrambled content to unscrambled content.

In analyzing claim 10 as a whole, it is clear that claim 10 is directed towards a machine and transformation and as such is directed to statutory subject matter. Claims 11 – 15 and 30 depend from claim 10 and as such, are also directed to statutory subject matter.

Independent claim 16 recites a method for transferring secure content over a network. The network is a group of machines. In addition, in each of the steps of claim 16, there are elements (bold-highlighted) that explicitly recite *a machine that implements the claimed step.*

> **receiving** a request for content **at a first server** over a first network from a file requesting device, said request including an

encryption key known to a designated remote site;

      generating a first information containing an access code and a content key **at said first server** in response to said request for content by said file requesting device;

      transferring said first information item **to said designated remote site** having a file receiving device, wherein said access code and said content key are scrambled using said encryption key;

      receiving said access code **from said designated remote site** having said file receiving device; and

      transferring secure content **over a second network** after verification of said access code, wherein said secure content is encrypted using said content key.

Accordingly, claim 16, *taken as a whole*, is directed to statutory subject matter. Claims 17 – 28, and 31 depend from claim 16 and as such are also directed to statutory subject matter.

Claims 1-2, 4-5, 10-13, and 29-30 are rejected under 35 U.S.C. § 103(a).

Claims 1-2, 4-5, 10-13, and 29-30 are rejected under 35 U.S.C. § 103(a) as unpatentable over US 6,385,317 (hereinafter Rix) and further in view of US 2002/0032665 (hereinafter Creighton). Applicants respectfully traverse this rejection for at least the following reasons.

Rix

Rix is aimed at preventing the use of an unauthorized smart card in combination with a conditional access module (CAM) (col. 2, lines 47-50). When the smart card is inserted into the CAM, the CAM generates a random key C_i that is used to encrypt and decrypt communications between the smart card and the CAM (col. 1, lines 26 – 40). The CAM also generates a random number A. The CAM transmits the random key C_i and A to the smart card encrypted using the CAM's public key (col. 2, lines 54 – 56). The smart card decrypts the message using the CAM's private key (col. 2, lines 56 – 59) and transmits the number A to the CAM encrypted with C_i (col. 2, lines 59 – 62). When the CAM receives back the number A, it knows that the smart card is authorized (col. 2, lines 64 – 67). Once the smart card is authorized, the CAM

sends ECMs containing the encrypted control word to the smart card. The ECMs contain a control word that is encrypted using a service key. The service key is downloaded to the smart card through an entitlement management message (col. 2, lines 36 – 38). From then on, communications between the smart card and the CAM will carry the control word encrypted with the key C_i (col. 3, lines 4-7).

Rix does not disclose or suggest "receiving a first information item comprising an access code and a content key scrambled using a key known by said device, said access code generated by said at least one server in response to a request for a second information item provided by the content requester."

The Examiner contends that the first information item is shown in Rix by the transmission from the CAM to the smart card that contains *A* (an access code) and C_i (the content key). However, Rix does not teach or suggest that the *access code was generated by at least one server in response to a request for a second information item provided by the content requester.* The content requester is distinct from the device. In Rix, the access code is a randomly generated number that is generated by the CAM. The CAM generates the access code to authenticate the smart card when the smart card is inserted into the CAM. The CAM does not generate the access code in response to a request for a second information item provided by a content requester as explicitly recited in claim 1. Furthermore, the CAM is not a server nor does Rix recite a content requester and server connected to a network that functions as recited in claim 1.

Rix does not teach or suggest "transmitting said access code to a server hosting said second information item."
The Examiner contends that the access code corresponds to the random number *A*, the server corresponds to the CAM, and the second information item corresponds to an entitlement control message (ECM). The Examiner further contends that the transmitting step is shown in Rix by the smart card transmitting the access code *A* to the CAM so that the CAM can authenticate the smart card. Applicant respectfully disagrees since the CAM is not a server hosting said second information item. The CAM is a **module in a decoder** that is not connected to a network. By contrast, the server of claim 1 is connected to a network. Applicants submit that one skilled in the

art would not correlate the CAM described by Rix to the recited server.

Rix does not teach or suggest "receiving said second information item scrambled using said content key after said server hosting the second information item verifies said access code."

The Examiner contends that the second information item corresponds to the ECM, that the content key corresponds to C_i, and that the CAM corresponds to the server. The Examiner further contends that the receiving step is shown in Rix as the smart card receiving an ECM that is scrambled using C_i after the CAM verifies the random number A. Applicant respectfully disagrees. In Rix, the smart card decrypts the ECM with the service key. The service key is downloaded in the smart card's memory via an entitlement management message (EMM). Rix does not recite that the smart card decrypts the ECM with C_i rather the smart card decrypts the ECM with the service key. By contrast, the receiving step of claim 1 recites that the second information item is scrambled using the content key which was transmitted by the content requestor. Clearly, this receiving step is not disclosed in Rix.

Creighton

Creighton pertains to online transactions between parties where the parties use digital certificates to authenticate the identity of each party. Once the identity of a party is authenticated, the authenticated party can obtain sensitive information. Creighton is focused on allowing a business owner, who has many potential business partners, to use an authentication server to authenticate potential business partners before permitting them to access commercial information from the business owner's website. The authentication server issues the business partner a digital certificate upon successful authentication which the business partner uses to access information from the business owner's website (paragraph [0043], Figs. 2 and 3).

The Examiner contends in the Office Action that "one of ordinary skill in the art at the time the invention was made would have been motivated to incorporate the structure of Creighton into the device of Fix to provide for an effective and efficient system of distributing tasks." Applicants respectfully disagree.

No motivation to combine Rix and Creighton

There is no motivation to combine Rix and Creighton to come up with the claimed invention. This is because each solves a different problem and the combination would not produce the claimed invention. Rix is concerned with the secure communication between a smart card and a CAM in order to prevent the switching of an authorized smart card with an unauthorized smart card. Creighton is concerned with authorizing business partners to access information from a central website accessible via the Internet with the use of digital certificates. These are entirely different environments having different considerations and problems.

By contrast, the claimed invention is concerned with allowing a content requester to send a request to a content server to download content to a device. The claimed invention ensures that both the content requester is authorized to make the request for the content and that the device is authorized to receive the content. In addition, the claimed invention ensures that the content is securely transmitted to an authorized device. Neither Rix nor Creighton address or solve this specific problem.

Furthermore, one skilled in the art would not be motivated to combine Rix and Creighton because they involve entirely different environments and address entirely different problems. The structure of Creighton relies on business parties communicating through online transactions communicated over a network. Rix pertains to secure communications between a smart card that is inserted into a CAM. The smart card and the CAM are not in communication with **a network**. As such, Rix is not suited or structured to operate in a network environment. Similarly, the solution of Creighton does not appear to apply in the smart card/CAM arrangement of Rix. One skilled in the art would not be motivated to incorporate the network structure of an online transaction processing scheme into a smart card that has no ability or need to receive communications through a network.

Accordingly, one skilled in the art would not look to these references since they address different problems, and thus, the features in the claimed invention are not recited, taught, or shown in these references.

11

Applicants submit that for at least the reasons discussed above, the suggested combination of Rix and Creighton fail to disclose, teach, or suggest each and every feature recited in the independent claims and the claims that depend on them, are believed to be patentably distinguishable over any combination of Rix and Creighton.

Claims 16-20, 23-27, and 31 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Rix and further in view of US Patent 7,392,393 (hereinafter Taki).

Claims 16-20, 23-27, and 31 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Rix and further in view of Taki. Applicants respectfully traverse this rejection since Taki is unable to remedy the deficiencies of Rix explained above in conjunction with claim 1. Accordingly, withdrawal of the rejection is respectfully requested.

Claims 3 and 6 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Rix, Creighton, and further in view of Ohmori (US 2004/0049464, hereinafter Ohmori).

Claims 3 and 6 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Rix, Creighton, and further in view of Ohmori. Applicants respectfully traverse this rejection since Ohmori is unable to remedy the deficiencies of Rix and Creighton explained above in conjunction with claim 1. Accordingly, withdrawal of the rejection is respectfully requested.

Claims 7-9 and 14-15 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Rix, Creighton, and further in view of Henrick (WO 02/32026A1, hereinafter Henrick).

Claims 7-9 and 14-15 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Rix, Creighton, and further in view of Henrick. Applicants respectfully traverse this rejection since Henrick is unable to remedy the deficiencies of Rix and Creighton explained above in conjunction with claim 1. Accordingly, withdrawal of the rejection is respectfully requested.

12

Claims 21 and 28 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Rix, Taki, and further in view of Henrick.

Claims 21 and 28 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Rix, Taki, and further in view of Henrick. Applicants respectfully traverse this rejection since Henrick is unable to remedy the deficiencies of Rix and Creighton explained above in conjunction with claim 1. Accordingly, withdrawal of the rejection is respectfully requested.

Claim 22 is rejected under 35 U.S.C. § 103(a) as being unpatentable over Rix, Taki, and further in view of Kuriya (US 2001/0056404, hereinafter Kuriya).

Claim 22 is rejected under 35 U.S.C. § 103(a) as being unpatentable over Rix, Taki, and further in view of Kuriya (US 2001/0056404, hereinafter Kuriya). Applicants respectfully traverse this rejection since Kuriya is unable to remedy the deficiencies of Rix and Taki explained above in conjunction with claim 1. Accordingly, withdrawal of the rejection is respectfully requested.

Conclusion

Having fully addressed the Examiner's rejections it is believed that, in view of the preceding amendments and remarks, this application stands in condition for allowance. Accordingly then, reconsideration and allowance are respectfully solicited.

It is believed that there are no additional fees due with regard to the filing of this response. However if there is an additional fee due, please charge the fee, or credit any overpayment, to Deposit Account No. 07-0832.

Respectfully submitted,
JUNBIAO ZHANG ET AL.

By: _____

Paul P. Kiel, Attorney
Reg. No. 40,677
Phone (609) 734-6815

Date: _8/18/10_

8/19/10
Patent Operations
Thomson Licensing LLC
P.O. Box 5312
Princeton, New Jersey 08543-5312